індивідуальні особливості ухвалення рішення людиною-експертом.

Реалізація принципу **вірогідності** експертної оцінки безпеки інформації в КС означає, що:

* для експертної оцінки повинні використовуватися різні методи прийняття рішень;
* забезпечується збіг результатів експертної оцінки при різних методах;
* використовуються неформальні методи оптимізації рішення для систем, де людина займає пріоритетне місце; при таких методах шукається не просто оптимальне рішення, а найбільш раціональне для визначених умов, факторів і параметрів системи для досягнення поставленої мети і придатне для широкого класу задач і умов експертної оцінки.

На **п'ятому рівні** ієрархії визначається, що можливими шляхами реалізації експертної оцінки безпеки інформації в КС можуть бути:

* розробка і використання для оцінки загальної методології безпеки інформаційних технологій; такий варіант реалізації експертної оцінки використовується в Єдиних міжнародних критеріях CCITSE, 1996–1997, що також покладені в основу міжнародного стандарту ISO/IEC 15408;
* методика експертної оцінки захищеності (безпеки) інформації від несанкціонованого доступу в комп'ютерних системах; така методика як нормативний документ Департаменту СТСЗІ СБУ поки на стадії розробки ;
* експертна оцінка безпеки інформації в КС із використанням експертних систем штучного інтелекту; досвід їхнього застосування показує, що вони найбільш перспективні для автоматизації і підвищення гарантії експертної оцінки;
* інші рішення експертної оцінки, до яких можна віднести перспективні і спеціальні методи, засоби автоматизованої підтримки прийняття рішень, наприклад, системи підтримки прийняття колективних рішень, конференції з прийняття рішень (decision conference), що, наприклад, уже використовуються Центром з прийняття рішень Лондонської школи економіки і політичних наук [5].

Таким чином, розглянуті шляхи рішення проблеми експертної оцінки безпеки інформації в комп'ютерних системах свідчать про те, що невирішених питань ще багато як у теоретичному, так і в практичному плані. Обговорення цієї проблеми в наступному доцільно продовжити.

*Література: 1. Пакет з п'яти нормативних документів щодо захисту інформації від несанкціонованого доступу, Департамент СТСЗІ СБ України, Київ, 1999 р. 2. Шорошев В. В., Ильницкий А. Е., Близнюк И. Л. Защита информации компьютерных систем от угроз НСД и национальные критерии ее экспертной оценки. Бизнес и безопасность № 6, 2000 г., с. 5–6. 3. Ж-л ББ-4-1998, с. 28–32, ББ-1-1999, с. 10–12. 4. Тарасов Г. П., Шорошев В. В., Ильницкий А. Е. Технологическая карта испытаний компьютерных систем на соответствие требованиям оцениваемого класса безопасности по международным критериям ITSEC, TCSEC. Бизнес и безопасность № 4, 1998 г., с. 28–32. 5. Ларичев О. И. Объективные модели и субъективные решения. Издательство ВНИИ системных исследований АН СССР "Наука", М., 1987.*

**УДК 681.3.06:519.248.681**

# АНАЛИЗ МЕТОДОВ И СРЕДСТВ ЗАЩИТЫ ОТ НСД

***Александр Замула, Виктор Руженцев***
*Харьковский национальный университет радиоэлектроники*
*Акционерное общество «ИИТ»*

*Анотація:* **Сформульовано концепцію забезпечення безпеки інформації в автоматизованих системах її обробки. Розглядаються основні проблеми, пов'язані з забезпеченням інформаційної безпеки. Оскільки сьогодні майже всі нові розробки систем обробки даних ведуться на основі ПЕОМ, однією з основних складових підсистеми інформаційної безпеки є підсистема захисту локальних робочих місць. Тому особлива увага приділяється саме цій підсистемі.**

*Summary:* **The main task of this report is to propose the conception of information security in automatized systems. The main problems of information security are considered in this report. Most of all modern information systems consist of local personal computers. That is why subsystem of security of local computers considered in report especially thoroughly.**

*Ключевые слова:* **Информационно-телекоммуникационные системы, несанкционированный доступ, локальная рабочая станция, программно-аппаратный комплекс, система защиты информации.**

В связи с высокой информатизацией общества проблема безопасности информации весьма актуальна. Однако решение этой проблемы, несмотря на большой объем проведенных исследований, усложняется тем, что до настоящего времени в Украине и за рубежом отсутствуют единые общепринятые теория и концепция обеспечения безопасности информации в автоматизированных системах ее обработки. В этой связи актуальной представляется задача создания концепции обеспечения безопасности информации в автоматизированных системах ее обработки, а также анализ средств защиты от несанкционированного доступа (НСД).

Проблемы, связанные с обеспечением информационной безопасности в современных информационно-телекоммуникационных системах (ИТС), обычно включают:

- защиту информационных ресурсов локальной рабочей станции (ЛРС) от НСД;
- защиту в локальных сетях передачи данных;
- защиту межсетевого взаимодействия;
- защиту электронной почты и документооборота;
- защиту электронных платежных систем.

Подсистема информационной безопасности (ПИБ) включает в себя весь комплекс средств и мер по защите информации ИТС. В ПИБ каждому классу средств и мер защиты информации выделяется своя задача, в связи с чем ряд средств и мер объединяются в подсистемы, которые (каждая по отдельности) решают строго определенные задачи, но при этом соблюдаются цели создания ПИБ и принципы ее построения. Типовая ПИБ может иметь следующую структуру:

- подсистема защиты локальных рабочих мест;
- подсистема защиты локальных вычислительных сетей (ЛВС);
- подсистема защиты межсетевого взаимодействия;
- подсистема аудита и мониторинга;
- подсистема технологической защиты.

Поскольку в настоящее время широкое распространение получили ПЭВМ и почти все новые разработки систем обработки данных ведутся на их основе, одной из основных составляющих подсистемы информационной безопасности является подсистема защиты локальных рабочих мест. Под локальной рабочей станцией понимается персональный компьютер при условии, что он не подсоединён к каналам передачи данных. Любая защита в современных информационных системах начинается, прежде всего, с конкретного рабочего места. Круг вопросов, связанных с обеспечением его безопасности, занимает одно из первых мест по остроте стоящих задач и по разнообразию средств и методов защиты ЛРС. Защита ЛРС особенно актуальна ещё и потому, что по статистике большинство нарушений в современных информационных системах приходится именно на внутренних нарушителей и происходит при помощи штатных средств.

Защита ЛРС – задача комплексная, состоящая из широкого круга проблем, решение которых возможно только после разработки общей для системы политики безопасности (ПБ). Разработка ПБ на первой стадии включает в себя тщательный анализ возможных угроз.

Угрозы можно классифицировать по следующим принципам:

I) по характеру доступа нарушителя:

1) с доступом к ПО;
2) с доступам только к аппаратным ресурсам;
3) без доступа к ЛРС;

II) по характеру проявления:

1) активные;
2) пассивные;

III) по используемым в ходе реализации угрозы средствам:

1) с использованием штатных средств, входящих в ЛРС;
2) с использованием дополнительных средств.

Перечень угроз приводится во многих источниках, например в [1, 2]. Создание защищённой системы – задача комплексная, и решается она путём применения программно-технических методов и средств, а также с помощью организационных мероприятий. В соответствии с возможными угрозами, предлагается следующий перечень мероприятий по защите данных:

1) обеспечение конфиденциальности и достоверности пользовательской информации;

2) разграничение доступа пользователей к информации, хранящейся и обрабатываемой на ЛРС при применении многопользовательского режима;

3) аутентификация пользователей и авторизация доступа к защищаемым объектам;

4) контроль целостности секретной пользовательской или системной информации;

5) контроль процесса загрузки ОС;

6) контроль целостности аппаратных ресурсов;

7) исключение негативного влияния на процесс функционирования пользовательского приложения со стороны программного окружения, установленного на ЛРС;

8) контроль запуска задач пользователем (пользователю для запуска должны быть доступны только те задачи, которые являются разрешёнными в рамках выбранной ПБ);

9) защита от побочного ЭМИ и утечки информации по цепям питания и заземления;

10) физическое удаление остаточной информации, возникающей в ходе функционирования ПО;

11) аудит и протоколирование работы средств защиты информации (СЗИ), системного и прикладного ПО.

Средства защиты информации, которые сегодня применяются и позволяют решать одну или несколько из перечисленных задач обеспечения информационной безопасности ЛРС, можно разделить на программные, аппаратные и программно-аппаратные.

Следует выделить программно-аппаратные решения по обеспечению защиты ЛРС, так как они позволяют совместить в себе преимущества аппаратной (высокая скорость, защищенность от утечки информации через побочные электромагнитные излучения и наводки) и программной (гибкость и переносимость) реализаций, а также устранить присущие в отдельности программной или аппаратной реализациям недостатки. Так, использование аппаратно-программных средств защиты информации позволяет вынести некоторые, особенно критичные к негативному воздействию процедуры, осуществляемые в данном средстве защиты, для реализации в аппаратной части, что заметно повышает уровень защиты информации. Например, функции подсчета контрольных сумм защищаемых файлов реализуются в аппаратной части, где и хранятся выработанные значения этих сумм.

Рассмотрим, как при помощи программно-аппаратных комплексов (ПАК) могут быть решены поставленные перед подсистемой защиты ЛРС задачи.

1) Обеспечение конфиденциальности и достоверности пользовательской информации реализуется путём применения средств шифрования и ЭЦП, выполненных как в виде абонентского шифрования (отдельная программа-вызов, запуск которой предоставляет пользователю возможность применять функции шифрования и ЭЦП), так и в виде средств прозрачного шифрования. Например, вызовы функций шифрования встраиваются в используемое пользовательское ПО, в ходе работы которого незаметно («прозрачно») для пользователя происходит вызов этих функций из прикладного ПО. При этом, алгоритмы шифрования и ЭЦП могут быть реализованы аппаратно, что позволяет гарантировать целостность алгоритма криптографического преобразования, повысить скорость выполнения преобразований, загружать ключи шифрования до запуска операционной системы в регистры шифропроцессора и хранить их там в процессе обработки файлов без выгрузки в оперативное запоминающее устройство, что гарантирует сохранность ключей от несанкционированного доступа. Значительно повышает надежность ключей шифрования и электронной подписи встроенный аппаратный датчик случайных чисел. Желательно также, чтобы ПАК имел интерфейс к адаптеру смарт-карт и (или) к коннектору touch-memory, что позволило бы хранить ключи шифрования на смарт-картах и (или) «таблетках» touch-memory.

2) В целях разграничения доступа пользователей к информации часто используются штатные средства ОС. Вследствие недостатков в их реализации, часто возникает желание иметь более надёжную защиту от НСД, что приводит к необходимости применения дополнительных средств разграничения доступа. Организация доступа к какой-либо информации, будь то файлы, директории или логические диски, может быть организована по уровням конфиденциальности. Например, каждому логическому диску присваивается уровень конфиденциальности, а каждому пользователю уровень доступа. Пользователю доступ к диску разрешается, если уровень конфиденциальности не превышает уровня доступа. Списки идентификаторов и другую информацию, касающуюся СЗИ, желательно хранить во внутренней, энергонезависимой памяти ПАК.

3) Аутентификация пользователей и авторизация доступа к защищаемым объектам может производиться с использованием криптографических методов или индивидуальных носителей (touch memory, смарт- карты, гибкие магнитные диски). Процедуры идентификации, аутентификации пользователя желательно проводить до загрузки операционной системы, например, путем перехвата управления во время так называемой процедуры ROM-SCAN. Суть процедуры заключается в том, что BIOS после проверки основного оборудования и проверки контрольной суммы ПЗУ производит вызов стандартной процедуры инициализации, которая находится по определенному адресу ПЗУ. Эта процедура может быть заменена. В результате, если пользователь не идентифицирован или не аутентифицирован, то возврата из процедуры не происходит, и дальнейшая загрузка выполняться не будет. Список идентификаторов желательно хранить в энергонезависимой памяти ПАК. Для проведения процедуры аутентификации должен быть предусмотрен режим ввода пароля в скрытом виде – в виде символов <*>.

4) Контроль целостности секретной пользовательской или системной информации реализуется путём применения программ, выполняющих функции генерации контрольных сумм и их проверки, бесключевые хеш-функции или имитовставки. Контроль целостности информации предполагает систематичность её проведения. Например, либо администратор безопасности должен инициировать её с помощью организационных мер, либо в прикладное или системное ПО должны быть встроены функции, реализующие контроль целостности, которые автоматически вызываются ПО непосредственно перед тем, как приступить к работе с защищаемой информацией. В этом случае запуск драйвера, работающего с ключами пользователя, должен происходить с предварительным контролем его целостности, или контролем целостности критичных системных файлов (файлов настроек, системных драйверов и т. д.) перед их загрузкой в память или передачей им управления.

5) Должна быть обеспечена загрузка строго определённой версии ОС и блокирована несанкционированная загрузка с внешних носителей или из сети. Особое внимание следует уделить тому, чтобы во время осуществления контрольных процедур (идентификация, аутентификация пользователя, проверка целостности) была блокирована загрузка ОС в обход этих процедур с диска А.

6) Контроль целостности аппаратных ресурсов необходимо осуществлять непосредственно перед тем, как пользователь начнёт работать с ЛРС. Если зафиксировано несанкционированное изменение аппаратной части или конфигурации аппаратной части ЛРС, работа с данной ЛРС должна блокироваться.

7) Исключение негативного влияния на процесс функционирования пользовательского приложения со стороны программного окружения, установленного на ЛРС (программное окружение – другое прикладное ПО, которое работает на данной ЛРС). Задача актуальна в многопользовательских системах, где один зарегистрированный пользователь, являющийся нарушителем, может реализовать программу, которая будет стартовать во время работы другого пользователя, при этом злоумышленник будет иметь возможность получать доступ к конфиденциальной информации. Данная задача решается с помощью контроля целостности ядра ОС и гарантии отсутствия программ-закладок в системах ПО. Хотя гарантировать отсутствие закладок очень сложно и практически невозможно, так как на сегодняшний день ПО, установленное на ЛРС, чаще всего зарубежного производства.

8) Контроль запуска задач пользователем подразумевает то, что пользователю для запуска должны быть доступны только те задачи, которые являются разрешёнными в рамках выбранной ПБ. Задача может решаться так: администратор определяет перечень разрешенных к запуску на компьютере программ, они подписываются электронной цифровой подписью администратора и проверяются на целостность при запуске.

9) Задачи защиты от побочного ЭМИ и утечки информации по цепям питания и заземления решаются путём анализа спектра излучения аппаратной части ЛРС, проведения специальных работ по экранированию, фильтрации побочных опасных сигналов или создания контролируемой территории, за пределами которой побочные излучения (сигналы) не представляют опасности в силу того, что их уровень ничтожно мал, чтобы можно было их зарегистрировать даже с помощью современных средств. Могут быть использованы генераторы шумов, позволяющие создавать высокий уровень помех, уловить за которыми несущий информацию сигнал затруднительно.

10) Проблемы физического удаления остаточной информации возникают в силу того, что прикладное и системное ПО создают временные файлы; в некоторых ОС существуют файлы подкачки, или страничные файлы, и не реализовано физическое затирание удаляемой информации. Следует заметить, что файлы подкачки могут содержать конфиденциальные данные в открытом виде, поэтому они часто являются наиболее уязвимыми местами в СЗИ.

11) Для осуществления аудита и протоколирования работы средств ЗИ, системного и прикладного ПО хорошая СЗИ должна вести журнал работы (доступный только администратору), в котором регистрируются следующие события:

- установка системы на компьютере;
- вход пользователя в систему;
- попытка доступа к запрещенному логическому диску;
- зашифрование/расшифрование/перешифровывание диска;
- добавление нового пользователя;
- смена полномочий пользователя;
- удаление пользователя;
- причины останова системы;
- попытка запуска неразрешенной программы;
- нарушение целостности разрешенной программы.

Таким образом, в результате проведенного анализа уязвимых мест ИТС, возможных каналов доступа (штатных и несанкционированных) к информационным ресурсам предложен ряд методов и мероприятий, позволяющих наиболее полно перекрыть известные угрозы, и даны рекомендации по организации выполнения этих мероприятий в программно-аппаратном исполнении ПИБ.

*Литература: 1. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. М. 2000. 2. Задірака В., Олексюк О. Методи захисту фінансової інформації. Київ: Вища школа, 2000. 3. Мельников Ю. Н. Защита информации в компьютерных системах. М.: Финансы и статистика; Электроинформ, 1997.*

**УДК 681.3**

# АНАЛИЗ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ И МЕТОДОВ ЗАЩИТЫ

***Александр Лаврентьев***
*НИЦ «ТЕЗИС» НТУУ «КПИ»*

*Аннотация*: **Приводится анализ составляющих технического канала утечки информации, классификация средств защиты, рассмотрен систематизированный подход к организации технической защиты информации.**
*Summary:* **The analysis of outflow, making the technical channel, of the information is resulted,Classification of means of protection, approach to organization of technical protection of the information.**
*Ключевые слова:* **Информация, утечка информации, технические каналы утечки информации**.

## I Место противодействия техническим разведкам в системе ТЗИ

С развитием информационных технологий основной угрозой для информации с ограниченным доступом (ИсОД) стала проблема несанкционированного доступа (НСД). Однако это не уменьшает опасности несанкционированного перехвата информации и по техническим каналам. Особенно это касается информационных систем, не имеющих выхода за пределы контролируемой территории. В этом случае для разведки нет альтернативы, кроме как использование технических средств перехвата информации.

Предлагается возможный вариант подхода к классификации технических каналов утечки информации и методов защиты, которые могут лечь в основу организации системы противодействия техническим разведкам.

## II Анализ структуры технических каналов утечки информации

По определению, технический канал утечки (ТКУ) информации представляет собой совокупность источника информации, среды распространения сигнала и разведаппаратуры (рис. 1).

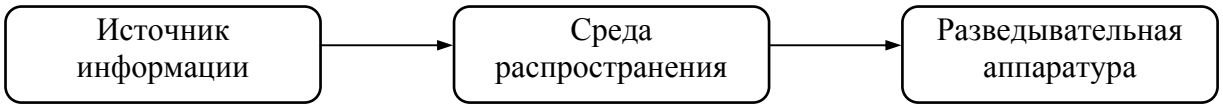


**Рисунок 1**

Это базовая схема технического канала утечки информации. Она не отражает существенных элементов процесса технической разведки. В конечном итоге разведывательные сообщества интересуют не поля, которые они перехватывают, а сведения, которые они могут получить на основании разведданных, полученных с помощью перехвата. Эти сведения не передаются напрямую, а претерпевают целый ряд преобразований, приводящих к возможности появления, распространения информационных полей и их перехвата и восстановления средствами технической разведки. С учетом этого ТКУ можно представить следующим образом (рис. 2).